PATENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Yasutaka NAGAO

Serial No. (unknown)

Filed herewith

NETWORK TRAFFIC MONITORING
SYSTEM AND MONITORING METHOD

CLAIM FOR FOREIGN PRIORITY UNDER 35 U.S.C. 119 AND SUBMISSION OF PRIORITY DOCUMENT

Assistant Commissioner for Patents

Washington, D.C. 20231

Sir:

Attached hereto is a certified copy of applicant's corresponding patent application filed in Japan on January 19, 2000 under No. 2000-009605.

Applicant herewith claims the benefit of the priority filing date of the above-identified application for the above-entitled U.S. application under the provisions of 35 U.S.C. 119.

Respectfully submitted,

YOUNG & THOMPSON

By _____

Robert J. Patch
Attorney for Applicant
Registration No. 17,355
745 South 23rd Street
Arlington, VA 22202
Telephone: 703/521-2297

January 18, 2001

後-出願
US

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２０００年　１月１９日

出願番号
Application Number: 特願２０００－００９６０５

出願人
Applicant (s): 日本電気株式会社

２０００年１２月　８日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号　出証特２０００－３１０１７２０

【書類名】　特許願
【整理番号】　47201430
【提出日】　平成12年 1月19日
【あて先】　特許庁長官殿
【国際特許分類】　H04L 12/00
【発明者】
　【住所又は居所】　東京都港区芝五丁目７番１号　日本電気株式会社内
　【氏名】　長尾　泰孝
【特許出願人】
　【識別番号】　000004237
　【氏名又は名称】　日本電気株式会社
【代理人】
　【識別番号】　100088812
　【弁理士】
　【氏名又は名称】　▲柳▼川　信
【手数料の表示】
　【予納台帳番号】　030982
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　ネットワークトラフィック監視システム及びそれに用いる監視方法

【特許請求の範囲】

【請求項１】　ＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）パケット毎にサービス単位に応じて優先度を変えて転送するＩＰネットワークにおいてトラフィック監視を行うネットワークトラフィック監視システムであって、前記トラフィック監視を前記サービス単位及び前記ＩＰネットワークのサブネットワーク単位で行う手段を有することを特徴とするネットワークトラフィック監視システム。

【請求項２】　ＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）ネットワークを構築するＩＰルータがリンクによって相互に接続され、ＩＰパケット転送の品質をクラス分けするＤｉｆｆｓｅｒｖ（ｄｉｆｆｅｒｅｎｔｉａｔｅｄ　ｓｅｒｖｉｃｅ）プロトコルに基づいてサービスクラス分けされたＩＰパケットの転送を行うネットワークにおいてトラフィック監視を行うネットワークトラフィック監視システムであって、前記リンク上を転送されるＩＰパケットを監視する手段と、その監視で検出されたＩＰパケットの前記サービスクラスを表す値と送出元ＩＰアドレス及び宛先ＩＰアドレスから割り出される送出元サブネットワークアドレスと宛先サブネットワークアドレスとに基づいてトラフィックを分類する手段と、その分類されたトラフィックを前記サービスクラス毎及び前記ＩＰネットワークのサブネットワーク毎に蓄積する手段とからなるトラフィックモニタ部を有することを特徴とするネットワークトラフィック監視システム。

【請求項３】　前記サービスクラスを表す値は、前記ＩＰパケットのヘッダ内フィールドの一部に前記サービスクラスを表す値を記録するためのフィールドとして割り当てられたＤＳＣＰ（Ｄｉｆｆｓｅｒｖ　Ｃｏｄｅ　Ｐｏｉｎｔ）を用いるようにしたことを特徴とする請求項２記載のネットワークトラフィック監視システム。

【請求項４】　前記サービスクラス毎及び前記サブネットワーク毎に蓄積さ

れたトラフィックデータに対して統計処理を施して前記トラフィックの表示と異常の監視とトレンドの把握とを行う監視マネージャを含むことを特徴とする請求項２または請求項３記載のネットワークトラフィック監視システム。

【請求項５】　前記監視マネージャは、前記サブネットワークのアドレス算出に必要なネットマスクを前記トラフィックモニタ部に供給するようにしたことを特徴とする請求項４記載のネットワークトラフィック監視システム。

【請求項６】　前記トラフィックモニタ部を前記ＩＰルータ内に配置したことを特徴とする請求項２から請求項５のいずれか記載のネットワークトラフィック監視システム。

【請求項７】　前記トラフィックは、ＭＩＢ（Ｍａｎａｇｅｍｅｎｔ　Ｉｎｆｏｒｍａｔｉｏｎ　Ｂａｓｅ）の形式で蓄積するようにしたことを特徴とする請求項２から請求項６のいずれか記載のネットワークトラフィック監視システム。

【請求項８】　ＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）パケット毎にサービス単位に応じて優先度を変えて転送するＩＰネットワークにおいてトラフィック監視を行うためのネットワークトラフィック監視方法であって、前記トラフィック監視を前記サービス単位及び前記ＩＰネットワークのサブネットワーク単位で行うようにしたことを特徴とするネットワークトラフィック監視方法。

【請求項９】　ＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）ネットワークを構築するＩＰルータがリンクによって相互に接続され、ＩＰパケット転送の品質をクラス分けするＤｉｆｆｓｅｒｖ（ｄｉｆｆｅｒｅｎｔｉａｔｅｄ　ｓｅｒｖｉｃｅ）プロトコルに基づいてサービスクラス分けされたＩＰパケットの転送を行うネットワークにおいてトラフィック監視を行うためのネットワークトラフィック監視方法であって、前記リンク上を転送されるＩＰパケットを監視し、その監視で検出されたＩＰパケットの前記サービスクラスを表す値と送出元ＩＰアドレス及び宛先ＩＰアドレスから割り出される送出元サブネットワークアドレスと宛先サブネットワークアドレスとに基づいてトラフィックを分類し、その分類されたトラフィックを前記サービスクラス毎及び前記ＩＰネットワークのサブネットワーク毎に蓄積するようにしたことを特徴とするネットワークトラフィック

監視方法。

【請求項１０】　前記サービスクラスを表す値は、前記ＩＰパケットのヘッダ内フィールドの一部に前記サービスクラスを表す値を記録するためのフィールドとして割り当てられたＤＳＣＰ（Ｄｉｆｆｓｅｒｖ　Ｃｏｄｅ　Ｐｏｉｎｔ）を用いるようにしたことを特徴とする請求項９記載のネットワークトラフィック監視方法。

【請求項１１】　前記サービスクラス毎及び前記サブネットワーク毎に蓄積されたトラフィックデータに対して統計処理を施して前記トラフィックの表示と異常の監視とトレンドの把握とを行うようにしたことを特徴とする請求項９または請求項１０記載のネットワークトラフィック監視方法。

【請求項１２】　前記ＩＰルータ内において、前記分類されたトラフィックを前記サービスクラス毎及び前記ＩＰネットワークのサブネットワーク毎に蓄積するようにしたことを特徴とする請求項９から請求項１１のいずれか記載のネットワークトラフィック監視方法。

【請求項１３】　前記トラフィックは、ＭＩＢ（Ｍａｎａｇｅｍｅｎｔ　Ｉｎｆｏｒｍａｔｉｏｎ　Ｂａｓｅ）の形式で蓄積するようにしたことを特徴とする請求項９から請求項１２のいずれか記載のネットワークトラフィック監視方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明はネットワークトラフィック監視システム及びそれに用いる監視方法に関し、特に大規模ＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）ネットワークにおけるトラフィック監視方法に関する。

【０００２】

【従来の技術】

従来、トラフィック監視手法においては、一般に、ＩＰヘッダ内から送信元ＩＰアドレスと宛先ＩＰアドレスとを読出し、これらのＩＰアドレスペアと４層宛先ポート番号とから識別される上位アプリケーション種別によって集計を行って

いる。

【０００３】

一方、ＩＥＴＦ（Ｉｎｔｅｒｎｅｔ　Ｅｎｇｉｎｅｅｒｉｎｇ　Ｔａｓｋ　Ｆｏｒｃｅ）によって新たなプロトコルとして、従来平等に転送されていたＩＰパケットに対して転送の優先度を設け、サービスに差別を設けるという技術が議論されるようになっている。これがＤｉｆｆｓｅｒｖ（ｄｉｆｆｅｒｅｎｔｉａｔｅｄ　ｓｅｒｖｉｃｅ）プロトコルである。

【０００４】

Ｄｉｆｆｓｅｒｖプロトコルに対応した端末や、Ｄｉｆｆｓｅｒｖサービスの境界となるルータでは、転送するＩＰパケットの送信元ＩＰアドレスや宛先ＩＰアドレス、使用するポート番号等によってパケットを数種類（ＩＥＴＦのＲＦＣ２４７５では、１４種のクラス）のサービスクラスに分類し、ＤＳＣＰ（Ｄｉｆｆｓｅｒｖ　Ｃｏｄｅ　Ｐｏｉｎｔ）としてＩＰヘッダ内に情報を埋め込んでパケット転送を行う。

【０００５】

Ｄｉｆｆｓｅｒｖプロトコルをサポートしたルータは、ＩＰヘッダ内に埋め込まれたＤＳＣＰの値を読込んで優先レベルを判断し、転送方法を決定するというアーキテクチャである。これによって、ＩＰパケットはクラス毎に分類された数種類のフローとして扱われ、特定のホストのＩＰパケットの廃棄率を低く設定したり、特定のアプリケーションパケットを低遅延で転送させたりすることが可能となる。

【０００６】

【発明が解決しようとする課題】

以上のようなネットワークに対し、従来のトラフィック監視方式においては、４層プロトコルのポート番号によってアプリケーション毎に総トラフィック量を分類しているので、Ｄｉｆｆｓｅｒｖプロトコルによって生ずる転送優先度を把握することができず、ネットワークがどのようなサービスに割り当てられているかを監視することができない。

【０００７】

また、Ｅｎｄ－ｔｏ－Ｅｎｄの端末同士でやりとりされるトラフィック量を分類しているので、ネットワークの規模が大きくなるにつれて扱うＩＰアドレス数が増加し、トラフィックモニタ部のメモリ容量圧迫や管理ネットワークへ負荷が増大するため、大規模ネットワークに対応しきれない。

【０００８】

さらに、ＩＰｓｅｃ（ｓｅｃｕｒｉｔｙ　ａｒｃｈｉｔｅｃｔｕｒｅ　ｆｏｒ　ｉｎｔｅｒｎｅｔ　ｐｒｏｔｏｃｏｌ）やＩＰｏｖｅｒＩＰのようなプロトコルを用いたネットワークでは４層プロトコルのポート番号を監視することができなくなるため、トラフィックをアプリケーション毎に分類することができない。

【０００９】

そこで、本発明の目的は上記の問題点を解消し、Ｄｉｆｆｓｅｒｖプロトコルを用いたＩＰネットワークにおいてネットワークの挙動を左右するサービス分布を把握することができ、大規模ネットワークにも対応することができるネットワークトラフィック監視システム及びそれに用いる監視方法を提供することにある。

【００１０】

【課題を解決するための手段】

本発明によるネットワークトラフィック監視システムは、ＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）パケット毎にサービス単位に応じて優先度を変えて転送するＩＰネットワークにおいてトラフィック監視を行うネットワークトラフィック監視システムであって、前記トラフィック監視を前記サービス単位及び前記ＩＰネットワークのサブネットワーク単位で行う手段を備えている。

【００１１】

本発明による他のネットワークトラフィック監視システムは、ＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）ネットワークを構築するＩＰルータがリンクによって相互に接続され、ＩＰパケット転送の品質をクラス分けするＤｉｆｆｓｅｒｖ（ｄｉｆｆｅｒｅｎｔｉａｔｅｄ　ｓｅｒｖｉｃｅ）プロトコルに基づいてサービスクラス分けされたＩＰパケットの転送を行うネットワークにおいてトラフィック監視を行うネットワークトラフィック監視システムであって、前記リンク

上を転送されるＩＰパケットを監視する手段と、その監視で検出されたＩＰパケットの前記サービスクラスを表す値と送出元ＩＰアドレス及び宛先ＩＰアドレスから割り出される送出元サブネットワークアドレスと宛先サブネットワークアドレスとに基づいてトラフィックを分類する手段と、その分類されたトラフィックを前記サービスクラス毎及び前記ＩＰネットワークのサブネットワーク毎に蓄積する手段とからなるトラフィックモニタ部を備えている。

【００１２】

本発明によるネットワークトラフィック監視方法は、ＩＰ（Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ）パケット毎にサービス単位に応じて優先度を変えて転送するＩＰネットワークにおいてトラフィック監視を行うためのネットワークトラフィック監視方法であって、前記トラフィック監視を前記サービス単位及び前記ＩＰネットワークのサブネットワーク単位で行うようにしている。

【００１３】

本発明による他のネットワークトラフィック監視方法は、ＩＰ（Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ）ネットワークを構築するＩＰルータがリンクによって相互に接続され、ＩＰパケット転送の品質をクラス分けするＤｉｆｆｓｅｒｖ（ｄｉｆｆｅｒｅｎｔｉａｔｅｄ ｓｅｒｖｉｃｅ）プロトコルに基づいてサービスクラス分けされたＩＰパケットの転送を行うネットワークにおいてトラフィック監視を行うためのネットワークトラフィック監視方法であって、前記リンク上を転送されるＩＰパケットを監視し、その監視で検出されたＩＰパケットの前記サービスクラスを表す値と送出元ＩＰアドレス及び宛先ＩＰアドレスから割り出される送出元サブネットワークアドレスと宛先サブネットワークアドレスとに基づいてトラフィックを分類し、その分類されたトラフィックを前記サービスクラス毎及び前記ＩＰネットワークのサブネットワーク毎に蓄積するようにしている。

【００１４】

すなわち、本発明のネットワークトラフィック監視システムは、インタネットやイントラネットに代表されるＩＰネットワークにおいて、トラフィック監視をサービス単位及びサブネットワーク単位で行うことによって収集するデータを集

約させてデータ量を削減し、大規模ネットワーク監視に適した監視システムを提供することを特徴としている。

【００１５】

より具体的に、本発明のネットワークトラフィック監視システムは、ＩＰネットワークを構築するＩＰルータであるＮＥ（ネットワークエレメント）がリンクによって相互に接続されており、Ｄｉｆｆｓｅｒｖ（ｄｉｆｆｅｒｅｎｔｉａｔｅｄ　ｓｅｒｖｉｃｅ）プロトコルに基づいてクラス分けされたＩＰパケットの転送を行っている。

【００１６】

ＤｉｆｆｓｅｒｖプロトコルはＩＥＴＦによって議論されているＩＰパケット転送の品質をクラス分けするプロトコルであり、ＩＰヘッダ内のフィールドの一部をサービスクラスを表すＤＳＣＰ（Ｄｉｆｆｓｅｒｖ　Ｃｏｄｅ　Ｐｏｉｎｔ）を記録するためのフィールドとして割り当て、このフィールドに設定される１４種のＤＳＣＰ値にしたがってパケット毎に優先度を変えて転送するという方式である。

【００１７】

トラフィックモニタ部はリンク上を転送されるＩＰパケットを監視し、つまりパケットをキャプチャし、サービスクラスを表すＤＳＣＰの値と、送出元ＩＰアドレス及び宛先ＩＰアドレスから割り出される送出元サブネットワークアドレスと、宛先サブネットワークアドレスとに基づいてトラフィックを分類し、内部メモリに蓄積するための装置である。

【００１８】

蓄積されたトラフィックデータはＳＮＭＰ（Ｓｉｍｐｌｅ　Ｎｅｔｗｏｒｋ　Ｍａｎａｇｅｍｅｎｔ　Ｐｒｏｔｏｃｏｌ）等を用いて監視マネージャへ転送されて統計処理が施され、トラフィックの表示・異常の監視・トレンドの把握等に用いられる。監視マネージャではサブネットワークアドレス算出に必要なネットマスクを入力するためのユーザインタフェースも提供する。

【００１９】

このようにして、本発明ではトラフィック監視の粒度としてサービスクラス毎

及びサブネットワーク毎に集計を行っているので、ネットワーク上の全端末同士で交換されるトラフィック情報を全アプリケーション毎に把握する代わりに、サブネットワーク毎・サービスクラス毎のトラフィックとして集約させた形で捉えることが可能となり、トラフィックモニタ部に必要なメモリ量を節約したり、監視マネージャへの通信量を低くすることが可能となる。

【００２０】

また、このようにして得られる集約されたトラフィックデータは、特に大規模ネットワークにおいてトラフィック管理をマクロ的に行う場合に有効な情報であることは言うまでもない。

【００２１】

よって、Ｄｉｆｆｓｅｒｖプロトコルを用いたＩＰネットワークにおいて、トラフィック監視の集計をサービス単位及びサブネットワーク単位で収集することで情報を集約させて監視することによって、ネットワークの挙動を左右するサービス分布を把握し、かつ大規模ネットワークにも対応可能となる。

【００２２】

【発明の実施の形態】

次に、本発明の実施例について図面を参照して説明する。図１は本発明の一実施例によるネットワークトラフィック監視システムの構成を示すブロック図である。図１において、ＮＥ（ネットワークエレメント）１，２はＩＰネットワークを構築するＩＰルータであり、リンク１００によって相互に接続されており、Ｄｉｆｆｓｅｒｖ（ｄｉｆｆｅｒｅｎｔｉａｔｅｄ　ｓｅｒｖｉｃｅ）プロトコルに基づいてクラス分けされたＩＰパケットの転送を行っている。

【００２３】

ＤｉｆｆｓｅｒｖプロトコルはＩＥＴＦによって議論されているＩＰパケット転送の品質をクラス分けするプロトコルであり、ＩＰヘッダ内のフィールドの一部をサービスクラスを表すＤＳＣＰ（Ｄｉｆｆｓｅｒｖ　Ｃｏｄｅ　Ｐｏｉｎｔ）を記録するためのフィールドとして割り当て、このフィールドに設定される１４種のＤＳＣＰ値にしたがって、パケット毎に優先度を変えて転送するという方式である。

【００２４】

トラフィックモニタ部（プローブ）３はリンク１００上を転送されるＩＰパケットを監視し、つまりパケットをキャプチャし、サービスクラスを表すＤＳＣＰの値と、送出元ＩＰアドレス及び宛先ＩＰアドレスから割り出される送出元サブネットワークアドレスと、宛先サブネットワークアドレスとに基づいてトラフィックを分類し、内部メモリ（図示せず）に蓄積するための装置である。

【００２５】

蓄積されたトラフィックデータはＳＮＭＰ（Ｓｉｍｐｌｅ　Ｎｅｔｗｏｒｋ　Ｍａｎａｇｅｍｅｎｔ　Ｐｒｏｔｏｃｏｌ）等を用いて監視マネージャ４へ転送されて統計処理が施され、トラフィックの表示・異常の監視・トレンドの把握等に用いられる。監視マネージャ４ではサブネットワークアドレス算出に必要なネットマスクを入力するためのユーザインタフェースも提供する。

【００２６】

このようにして、本実施例ではトラフィック監視の粒度としてサービスクラス毎及びサブネットワーク毎に集計を行っているので、図示せぬネットワーク上の全端末同士で交換されるトラフィック情報を全アプリケーション毎に把握する代わりに、サブネットワーク毎・サービスクラス毎のトラフィックとして集約させた形で捉えることができ、トラフィックモニタ部３に必要なメモリ量を節約したり、監視マネージャ４への通信量を低くすることができる。

【００２７】

また、このようにして得られる集約されたトラフィックデータは、特に大規模ネットワークにおいてトラフィック管理をマクロ的に行う場合に有効な情報である。

【００２８】

図２は図１のトラフィックモニタ部３の構成を示すブロック図である。図２において、トラフィックモニタ部３はインタフェース部３１と、抽出部３２と、回析部３３と、制御部３４と、メモリ部（ＭＩＢ：Ｍａｎａｇｅｍｅｎｔ　Ｉｎｆｏｒｍａｔｉｏｎ　Ｂａｓｅ）３５と、ＳＮＭＰエージェント３６とから構成されている。

【００２９】

インタフェース部３１はネットワークリンク１００と接続され、ＩＰパケットのキャプチャを行い、物理層及びデータリンク層の終端を行う部分である。抽出部３２は下位層の終端が行われたＩＰヘッダから、集計に必要となるＤＳＣＰと送出元ＩＰアドレスと宛先ＩＰアドレスとをそれぞれ抽出する。

【００３０】

解析部３３は抽出された情報と制御部３４から受け渡されるネットマスクとからサービスクラス毎及びサブネットワーク毎のトラフィックを集計し、ＭＩＢの形式でメモリ部３５に蓄積を行う部分である。制御部３４はサブネットワークアドレス算出のためのネットマスクを監視マネージャ４からＳＮＭＰエージェント３６経由で設定したり、トラフィックモニタ部３全体の動作制御を行う部分である。ＳＮＭＰエージェント３６はトラフィックモニタ部３と監視マネージャ４との間のデータ交換に用いられる。

【００３１】

監視マネージャ４はＳＮＭＰプロトコルを用いてトラフィックモニタ部３にネットマスクを設定したり、定期的にトラフィックモニタ部３内のメモリ部３５にＭＩＢの形式で保存された収集データにアクセスを行って、このデータをさらに統計・加工処理してトラフィック状態を表示したり、データを蓄積して異常状態の監視やトレンドの把握を行う装置である。

【００３２】

以上、本実施例の構成について述べたが、監視マネージャ４は当業者にとってよく知られており、また本発明とは直接関係しないので、その詳細な構成及び動作についての説明は省略する。

【００３３】

図３は図２の抽出部３２へ送られるヘッダ情報の詳細を示す図である。図３（ａ）はＩＰｖ４（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ　ｖｅｒｓｉｏｎ　４）フォーマットのヘッダ情報を示し、図３（ｂ）はＩＰｖ６（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ　ｖｅｒｓｉｏｎ　６）フォーマットのヘッダ情報を示している。

【００３４】

図４は図２の解析部３３にて行う集計動作を説明するための図である。これら図１～図４を参照して本発明の一実施例によるネットワークトラフィック監視システムの動作について説明する。

【００３５】

まず、トラフィック監視に先立ち、監視マネージャ４からトラフィックモニタ部３に対してサブネットワーク算出に用いるネットマスクが設定される。ネットマスクはＩＰアドレスのホストアドレスを隠蔽するためのビット列であり、設定はビットを指定しても良いし、例えば（２５５．２５５．２５５．０）や（２５５．２５５．０．０）、（２５５．０．０．０）といったアドレスの形式としても良い。トラフィックモニタ部３はこれを制御部３４に記録しておく。

【００３６】

次に、トラフィックモニタ部３がリンク１００上を流れるＩＰパケットを受信した場合、インタフェース部３１では受信したＩＰパケットの物理層及びデータリンク層を終端し、ヘッダ情報を抽出部３２へ送る。

【００３７】

ここで、抽出部３２へ送られるヘッダ情報の詳細を図３に示す。図３（ａ）はＩＰｖ４フォーマットのヘッダ情報を示しており、ＩＰヘッダの先頭から２バイト目にＴＯＳ（Ｔｙｐｅ　ｏｆ　Ｓｅｒｖｉｃｅ）フィールド１１が、３バイト目にＬｅｎｇｔｈフィールド１３が、１３バイト目に宛先ＩＰアドレスフィールド１４が、１７バイト目に送出元ＩＰアドレスフィールド１５がそれぞれ位置している。ＤＳＣＰはＴＯＳフィールド１１にマッピングされている。

【００３８】

また、図３（ｂ）はＩＰｖ６フォーマットのヘッダ情報を示しており、５ビット目にＴｒａｆｆｉｃ　Ｃｌａｓｓフィールド１２が、５バイト目にＬｅｎｇｔｈフィールド１３が、９バイト目に宛先ＩＰアドレスフィールド１４が、２５バイト目に送出元ＩＰアドレスフィールド１５がそれぞれ位置している。ＤＳＣＰはＴｒａｆｆｉｃ　Ｃｌａｓｓフィールド１２にマッピングされている。抽出部３２はこれらの情報を読取って解析部３３へと送る。

【００３９】

解析部３３は制御部３４から受け渡されたネットマスクと、ＩＰヘッダから抽出された宛先ＩＰアドレス及び送出元ＩＰアドレスとの和をとることによって、宛先サブネットワークと送出元サブネットワークとを算出し、このサブネットワークのペアと、同様にＩＰヘッダから抽出されたＤＳＣＰ値（すなわち、サービスクラス）毎にエントリを作成し、該当エントリについてＬｅｎｇｔｈフィールド１３で示されたＩＰパケット長、エントリを確認した回数（すなわち、該当ＩＰパケットの受信回数）それぞれの累積を、メモリ部３５にＭＩＢ情報として蓄積する。

【００４０】

次に、解析部３３にて行う集計動作について例を挙げて説明する。現在、監視マネージャ４からトラフィックモニタ部３に、（２５５．２５５．０．０）というネットマスクが設定されているものとする。

【００４１】

この状態において、トラフィックモニタ部３が送出元ＩＰアドレス（１０．２４．３２．１０１）から宛先アドレス（２０．３２．５２．２１１）に対して送られたＤＳＣＰ値（１０１１１０）のパケット長ＬのＩＰパケットを受信したとする。

【００４２】

このとき、トラフィックモニタ部３の解析部３３では、図４に示すようなエントリ２１ａを作成する。作成されたエントリ２１ａはパケット長Ｌとともにメモリ部３５内にレングスカウンタ３５ｂ、エントリカウンタ３５ｃとともに１つのレコード３５ａとして格納される。

【００４３】

エントリカウンタ３５ｃはレコード３５ａが生成された時に「１」であり、該当エントリが収集される毎に１ずつインクリメントされるカウンタで、すなわち該当ＩＰパケット通信個数を表す。レングスカウンタ３５ｂはキャプチャされる毎にパケットレングスが加算されるカウンタで、すなわち該当ＩＰパケットの通信オクテット数を表す。

【００４４】

続いて、送出元ＩＰアドレス（１０．２４．３３．１０）から宛先アドレス（２０．３２．５２．２００）に対して送られたＤＳＣＰ値（１０１１１０）のパケット長MのＩＰパケットを受信したとする。このパケットのエントリは先に作られたエントリ２１ａのものと一致するので、エントリカウンタ３５ｃは「２」となり、レングスカウンタ３５ｂは「Ｌ＋Ｍ」となる。

【００４５】

また、送出元ＩＰアドレス（１０．２４．３３．１０）から宛先アドレス（２０．３２．５２．．２１１）に対して送られたＤＳＣＰ値（００１０１０）のパケット長MのＩＰパケットを受信したとする。この場合、サブネットアドレスは先に送られているＩＰパケットと一致するが、ＤＳＣＰが異なるため、新たなエントリ２１ｂとしてメモリ部３５に格納される。

【００４６】

このように、従来方式のように個々のＩＰアドレスでエントリを作成した場合、ｎ台のホストがある状況では最大でｎ×（ｎ－１）個のエントリを作成しなければならず、また４層ポート番号によってプロトコルの識別を行っているため、使用されるポート番号の個数に比例したエントリがさらに必要となる。

【００４７】

一方、本実施例のようにサービス毎・サブネットワーク毎に集計を行えば、プロトコルは１４種のサービスのいずれかに分類されるため、サブネットワークがm個（m＜ｎ）である場合、エントリは最大でもｍ×（ｍ－１）×１４個だけ作成されることになる。

【００４８】

よって、本実施例ではサービス毎・サブネットワーク毎に集計を取っているので、プロトコル毎・Ｅｎｄ－ｔｏ－Ｅｎｄの端末毎に情報を蓄積する場合に比べて情報量が少なくなり、トラフィックモニタ部３のメモリを節約することができる。

【００４９】

また、本実施例ではサービス毎・サブネットワーク毎に集計を取っているので

、大規模ネットワークに対しても監視の適用が可能となる。エントリ数はｎやｍの２乗に比例するので、ｎとｍとの差が大きければ大きいほど、つまり大規模ネットワークほど効果が大きく表れる。

【００５０】

さらに、本実施例ではサービス毎・サブネットワーク毎に集計を取っているので、監視マネージャ４へ転送する情報も少なくなるため、管理ネットワーク上の通信負荷を削減することができる。

【００５１】

さらにまた、抽出する情報が全てＩＰヘッダ上にあるため、ＩＰｓｅｃ（ｓｅｃｕｒｉｔｙ ａｒｃｈｉｔｅｃｔｕｒｅ ｆｏｒｉｎｔｅｒｎｅｔ ｐｒｏｔｏｃｏｌ）のＥＳＰ（Ｅｎｃａｐｓｕｌａｔｉｏｎ Ｓｅｃｕｒｉｔｙ Ｐａｙｌｏａｄ）やＩＰｏｖｅｒＩＰのようなカプセル化プロトコルを用いたネットワークに対しても、サービスレベルでのトラフィック監視が可能となる。

【００５２】

従来方式では上記のＩＰｓｅｃやＩＰｏｖｅｒＩＰプロトコルが用いられたネットワークにおいて、４層ポート番号が暗号化されたり、ヘッダ先頭からの位置が変化してしまうので、情報を抽出することができず、トラフィックをプロトコル毎に分類することができない。

【００５３】

一方、本実施例のようにＤＳＣＰに基づいたサービス毎のトラフィック集計はカプセル化外部のＩＰヘッダ内にその情報が含まれるため、その監視を行うことができる。また、Ｄｉｆｆｓｅｒｖプロトコルを用いたネットワークにおいては、各種アプリケーションによって分類されたトラフィック情報よりも、転送優先度に基づいて分類されたトラフィック情報の方が、ネットワークのＱｏＳ（Ｑｕａｌｉｔｙ ｏｆ Ｓｅｒｖｉｃｅ）を端的に表現することができるため、付加価値の高い情報として扱うことができる。本実施例では以上の効果から、監視システム全体としての監視性能向上が見込まれる。

【００５４】

上記の監視マネージャ４からトラフィックモニタ部３に設定するネットマスク

は自由に設定可能であるため、（２５５．２５５．２５５．２５５）のようなマスクを設定した場合、サブネットワークアドレスがホストＩＰアドレスと等しくなり、従来のようなＥｎｄ－ｔｏ－Ｅｎｄ毎のトラフィック監視も可能となる。

【００５５】

図５は本発明の他の実施例によるルータの構成を示すブロック図である。図５においては本発明の他の実施例によるルータ５内部にトラフィックモニタ部５１を組込んだ例を示している。

【００５６】

ルータ５のインタフェース＃１～＃ｎからなるインタフェース部３１に到着したパケットのヘッダ情報はフォワーディングエンジン部５２へ転送され、宛先ＩＰアドレスからハードウェア的に送出先が検索される。このヘッダ情報を抽出部３２にもフォワーディングエンジン部５２と同様に受け渡すことによって、ルータ５のインタフェース部３１に関わらずトラフィックを収集することができるようになる。よって、ノードにおけるトラフィック監視が可能となる。

【００５７】

この形態において、（０．０．０．０）のようなマスクを設定した場合には、図示せぬネットワーク内のサービス分布（どのノードにどのサービスが集中しているか等）を把握することも可能となる。

【００５８】

また、上記の形態において、トラフィックモニタ部５１と監視マネージャ（図示せず）との間の通信にＣＯＰＳ（Ｃｏｍｍｏｎ　Ｏｐｅｎ　Ｐｏｌｉｃｙ　Ｓｙｓｔｅｍ）プロトコルを用いた場合には、トラフィックモニタ５１部と監視マネージャ部との信頼性の高い通信や、監視ポリシーの設定を実現することができる。ＣＯＰＳプロトコルを利用する場合にはポリシー受け渡しのためのクライアントタイプを予め設定しなければならないが、トラフィックモニタのためのクライアントタイプはＩＥＴＦでも決定はされていないため、新たなクライアントタイプとして登録を行う。

【００５９】

【発明の効果】

以上説明したように本発明によれば、ＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）パケット毎にサービス単位に応じて優先度を変えて転送するＩＰネットワークにおいてトラフィック監視を行うネットワークトラフィック監視システムにおいて、トラフィック監視をサービス単位及びＩＰネットワークのサブネットワーク単位で行うことによって、Ｄｉｆｆｓｅｒｖプロトコルを用いたＩＰネットワークにおいてネットワークの挙動を左右するサービス分布を把握することができ、大規模ネットワークにも対応することができるという効果がある。

【図面の簡単な説明】

【図１】

本発明の一実施例によるネットワークトラフィック監視システムの構成を示すブロック図である。

【図２】

図１のトラフィックモニタ部の構成を示すブロック図である。

【図３】

（ａ）はＩＰｖ４フォーマットのヘッダ情報を示す図、（ｂ）はＩＰｖ６フォーマットのヘッダ情報を示す図である。

【図４】

図２の解析部にて行う集計動作を説明するための図である。

【図５】

本発明の他の実施例によるルータの構成を示すブロック図である。

【符号の説明】

１，２　ＮＥ

３，５１　トラフィックモニタ部

４　監視マネージャ

５　ルータ

１１　ＴＯＳフィールド

１２　Ｔｒａｆｆｉｃ　Ｃｌａｓｓフィールド

１３　Ｌｅｎｇｔｈフィールド

１４　宛先ＩＰアドレスフィールド

１５　送出元ＩＰアドレスフィールド

２１ａ，２１ｂ　エントリ

３１　インタフェース部

３２　抽出部

３３　回析部

３４　制御部

３５　メモリ部

３５ａ　レコード

３５ｂ　レングスカウンタ

３５ｃ　エントリカウンタ

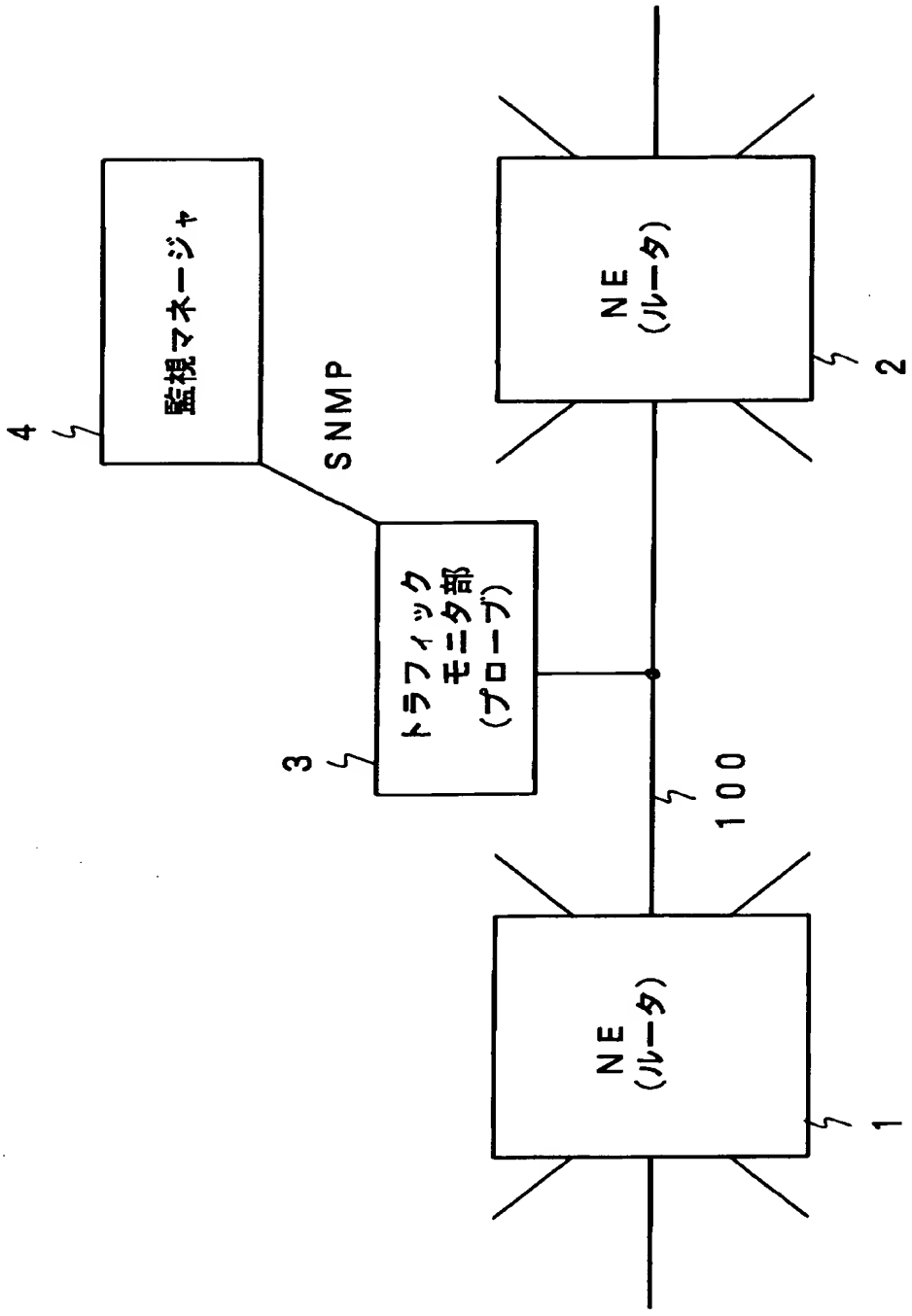
３６　ＳＮＭＰエージェント

５２　フォワーディングエンジン部

１００　リンク

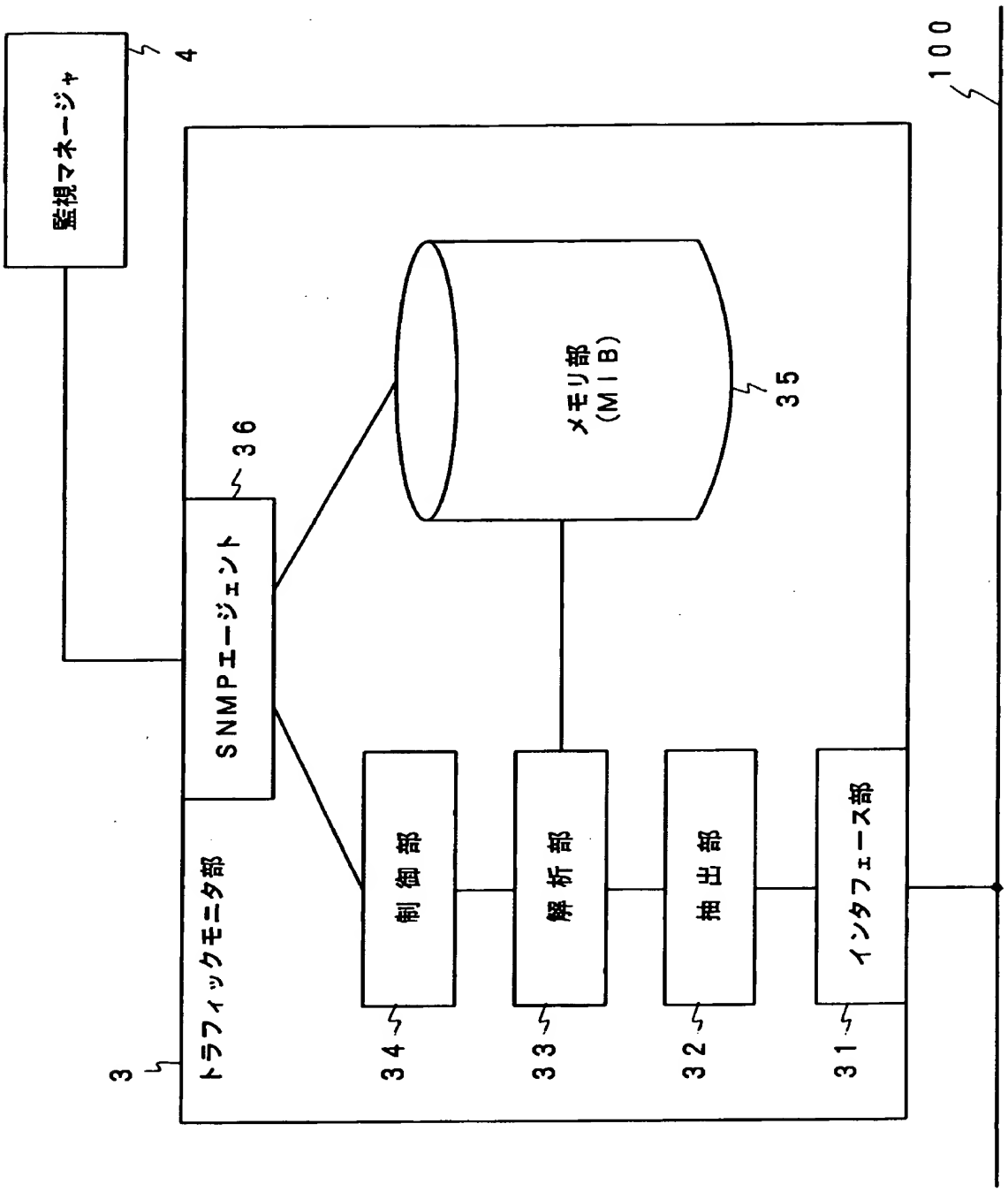
【書類名】　　図面

【図１】

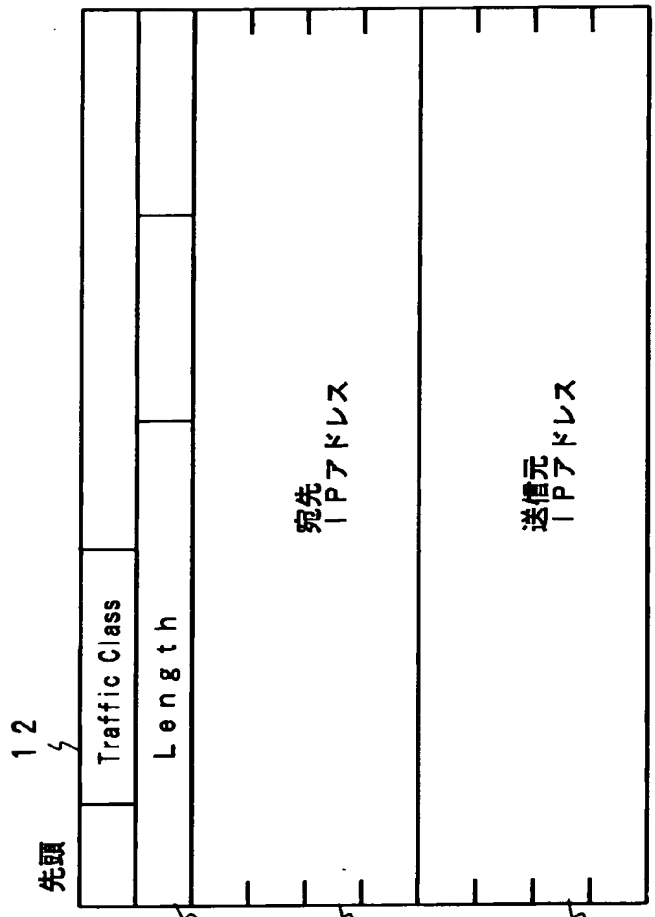


出証特２０００－３１０１７２０

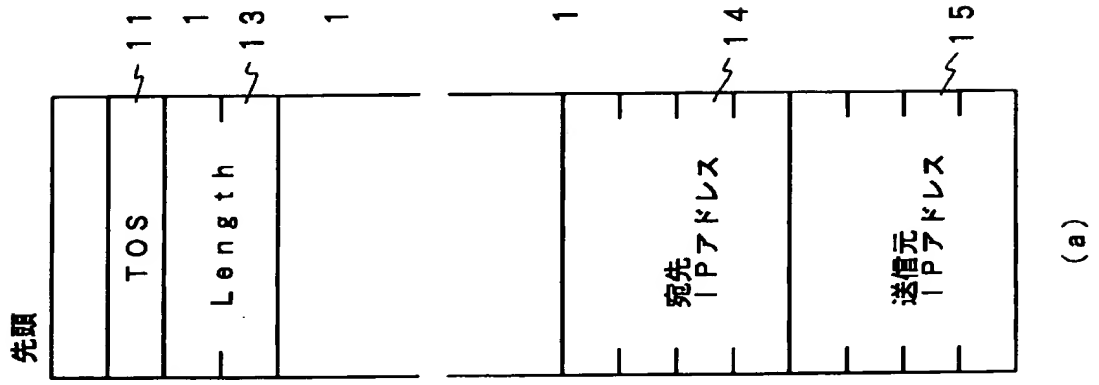
【図２】

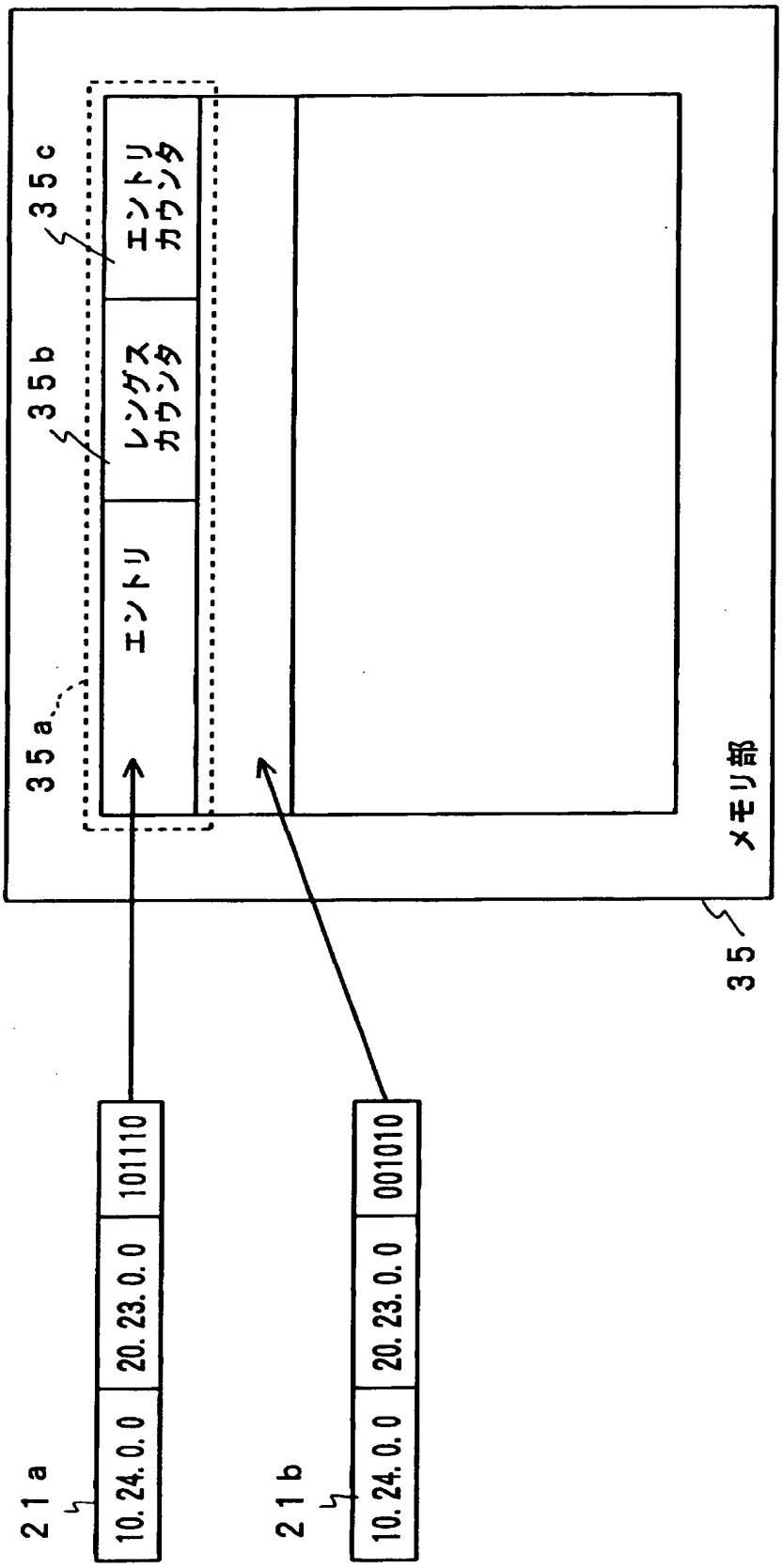

監視マネージャ
4
100
メモリ部
(MIB)
35
36
SNMPエージェント
トラフィックモニタ部
3
収集部
解析部
抽出部
インタフェース部
34
33
32
31

【図３】

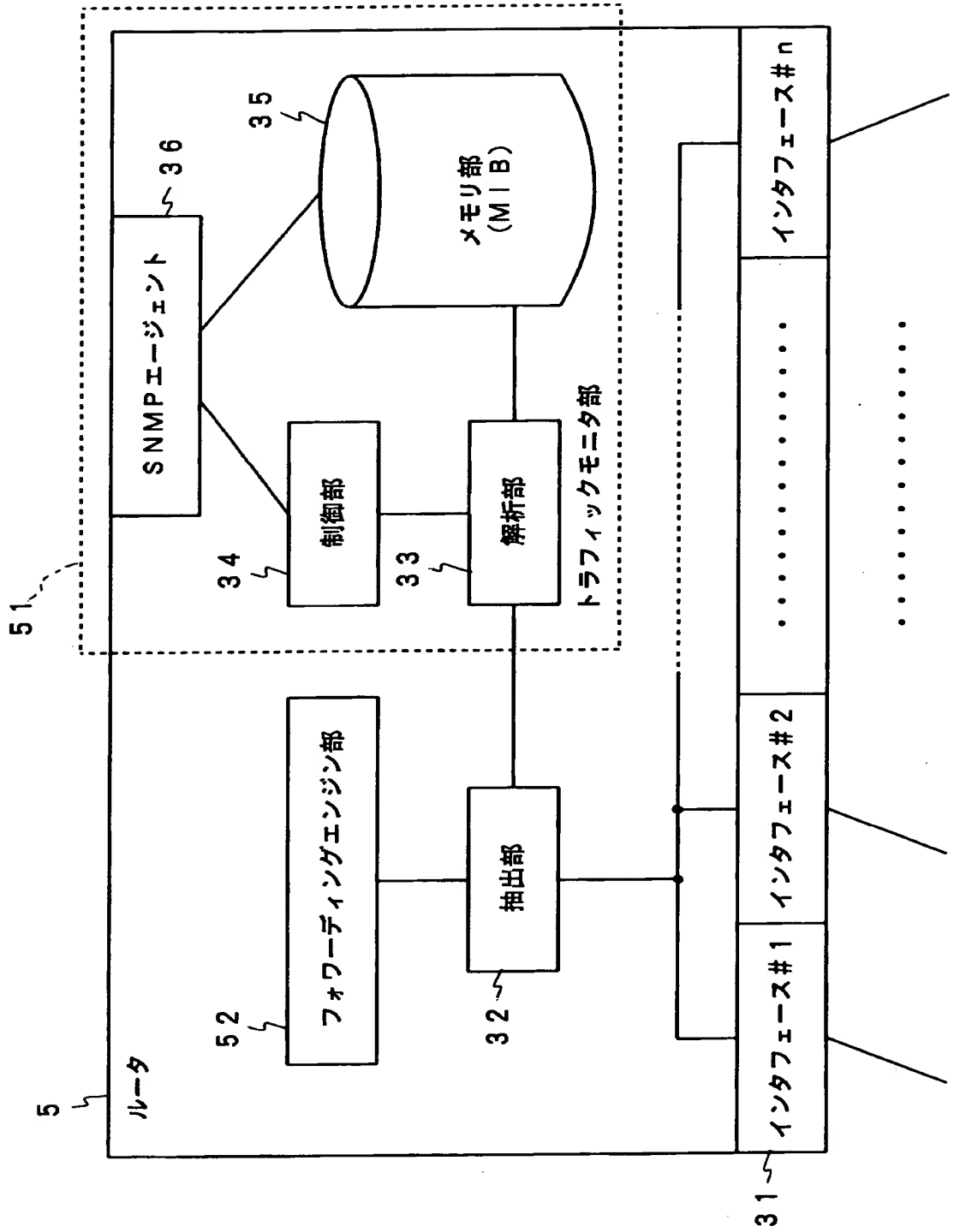

先頭
12
Traffic Class
Length
宛先IPアドレス
送信元IPアドレス
(b)
11
13
14
15

【図４】


先頭
TOS
Length
宛先IPアドレス
送信元IPアドレス
(a)
11
13
14
15


35c
エントリカウンタ
35b
レングスカウンタ
エントリ
35a
メモリ部
35
21a
10.24.0.0
20.23.0.0
101110
21b
10.24.0.0
20.23.0.0
001010

【図５】


ルータ
5
フォワーディングエンジン部
52
抽出部
32
制御部
34
解析部
33
トラフィックモニタ部
51
SNMPエージェント
36
メモリ部
(MIB)
35
インタフェース#1
インタフェース#2
インタフェース#n
31

【書類名】　　要約書

【要約】

【課題】　Ｄｉｆｆｓｅｒｖプロトコルを用いたＩＰネットワークにおいてネットワークの挙動を左右するサービス分布を把握し、大規模ネットワークにも対応可能なネットワークトラフィック監視システムを提供する。

【解決手段】　インタフェース部３１はＩＰパケットのキャプチャを行い、物理層及びデータリンク層の終端を行う。抽出部３２はＩＰヘッダから集計に必要となるＤＳＣＰと送出元ＩＰアドレスと宛先ＩＰアドレスとを抽出する。解析部３３は抽出された情報とネットマスクとからサービスクラス毎及びサブネットワーク毎のトラフィックを集計し、ＭＩＢの形式でメモリ部３５に蓄積する。制御部３４はサブネットワークアドレス算出のためのネットマスクを監視マネージャ４からＳＮＭＰエージェント３６経由で設定し、トラフィックモニタ部３全体の動作制御を行う。

【選択図】　　図２

出　願　人　履　歴　情　報

識別番号　　〔０００００４２３７〕

１．変更年月日　　１９９０年　８月２９日
［変更理由］　新規登録
住　所　東京都港区芝五丁目７番１号
氏　名　日本電気株式会社